PART5　情報セキュリティ

目標

- サイバー犯罪にはどのような種類があるか理解する。
- 情報セキュリティを確保する仕組みを理解する。
- 情報セキュリティを確保するために，具体的にできることを考えられるようになる。

Chapter1　情報セキュリティ

サイバー犯罪

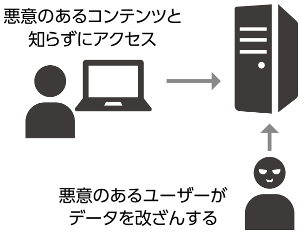
〔①　　　　　　　　　　〕：コンピュータおよびネットワーク技術を悪用した犯罪。インターネットの世界的な発展にともない，多様化･高度化を続けている。匿名性が高い，痕跡が残りにくい，不特定多数が被害を受ける，時空間の制約がない，などの特徴がある。

知っておこう

サイバー犯罪は，
(1) 不正アクセス禁止法違反
(2) コンピュータ・電磁気的記録対象犯罪
(3) その他
などに類型化される。「その他」としてはネットワーク利用犯罪などがある。

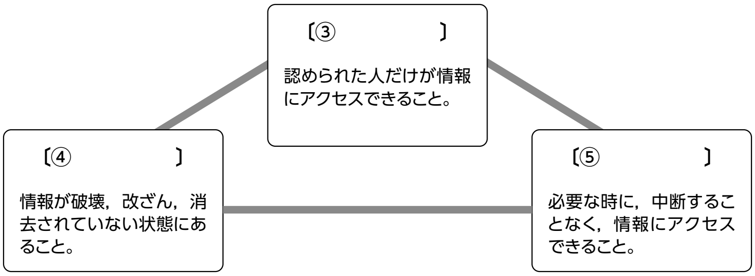
他人のIDとパスワードでログイン

データを改ざんする



情報セキュリティ

〔②　　　　　　　　　　　　〕：情報を適切に管理し，安全に保つこと。具体的には次の 3 つを維持することが重要となる。



知っておこう

機密性（Confidentiality），
完全性（Integrity），
可用性（Availability）
の頭文字を取って「情報セキュリティの CIA」と呼ばれることもある。

ここが POINT

情報セキュリティに関する技術の詳細は第 8 講で扱う。

情報セキュリティには，技術だけではなく，個人や組織による適切な対策が重要となる。

〔⑥　　　　　　　　　　　　　　〕：情報通信技術を使用せず，人の心理的な隙や行動のミスにつけこんで，パスワードなどを盗み出す方法。

知っておこう

パスワードクラッキング（本人以外によるパスワードの割り出し）には，次のような手法がある。

・ブルートフォース攻撃
総当たりで，全ての組み合わせを次々と試していく。

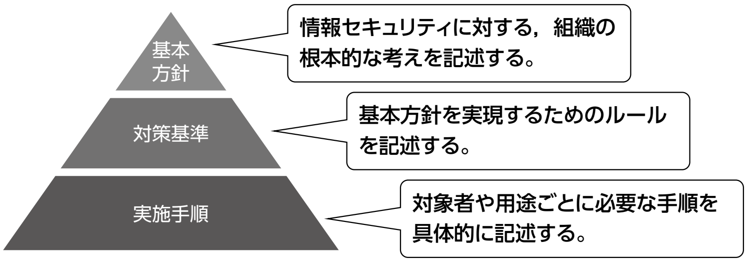
・ディクショナリー攻撃
辞書に掲載されている単語や，人物名などを次々に試していく。

・パスワードリスト攻撃
ほかの Web サイトから流出した ID とパスワードのリストをもとに試していく。

攻撃手法を知ることで，どのようなパスワードが安全であるか考えることができる。

• 組織でできること

〔⑦　　　　　　　　　　　　　〕：組織（企業や学校など）の持つ情報資産の安全性を保つために，組織が作成する対応策や規定。外部からの脅威への対応だけではなく，組織内部の情報管理についても規定する。



〔⑧　　　　　　　〕：コンピュータのファイルやフォルダ，周辺機器などに対して利用者ごとに与えられる権限。不必要な人間にはアクセス権を与えないことで，情報流出のリスクを下げることができる。

• 個人でできること

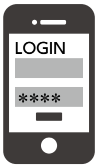
パスワードをより安全性の高いものに変更することも，対策のひとつである。〔⑨　　　　　　　　　　　　〕・〔⑩　　　　　　　　　　　　〕を避ける。

- **パスワード以外の認証方式**

〔⑪　　　　〕とは，対象（人やコンピュータ）の正当性や真正性を証明したり確認したりする行為である。

知識認証

その情報を知っていればログインできる認証のこと（例：ID とパスワードによる認証）

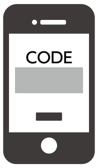


生体認証

身体的特徴や行動的特徴（癖）の情報を用いて行う認証（例：指紋認証）

所持認証

本人しか持っていない物で行う認証（例：スマートフォンに SMS で認証コードを送る方法）



〔⑫　　　　　　〕:「知識」「生体」「所持」の要素のうち，2 つの要素を組み合わせる認証。

知っておこう

身体的特徴の例として，指紋や顔, DNA, 目の網膜, 虹彩, 音声, 指の静脈などがある。
行動的特徴の例として，筆跡，まばたき，歩行などがある

知っておこう

2 つ以上の要素を組み合わせる認証を多要素認証という。つまり，二要素認証は多要素認証の一種である。また，指紋認証＋虹彩認証のように同一要素ではあるが 2 段階の認証を行うことは，「二段階認証」という。

- **継続的な管理**

情報セキュリティの確保には，継続的な管理が欠かせない。

〔⑬　　　　　　〕：コンピュータに何らかの被害を及ぼすように，悪意を持って作成された不正なソフトウェア。マルウェアによる被害を防ぐためにも，定期的なソフトウェアの〔⑭　　　　　　〕が重要になる。

知っておこう

マルウェアにはコンピュータウイルス，スパイウェア，ランサムウェアなどさまざまな種類がある。

重要

ウイルス対策ソフトウェアの導入も，マルウェア対策として有効である。

まとめ

- **サイバー犯罪**には，不正アクセスやデータの改ざん，ネットワークを利用した犯罪（脅迫など）といった種類がある。
- 情報を適切に管理し，安全に保つ**情報セキュリティ**の維持には，技術だけでなく，組織・個人による取り組みも重要になる。
- 定期的なソフトウェアのアップデートや，安全性の高いパスワードを使うことは個人として情報セキュリティを確保することにつながる。

＜MEMO＞

Chapter2　実践問題

問 1　あなたのスマートフォンの情報セキュリティを保つために，取り入れられる具体的な対策を列挙し，自分自身の情報セキュリティポリシーを作りましょう。

問 2　次の行為の何が危険か，この後どうなるか考えてみよう。

(1)

(2)

＜MEMO＞

第1講　PART5　確認問題

問１　情報セキュリティはある３つの要素を確保することだと定義されている。この３つの要素を表す語句の組み合わせとして最も適切なものを，次の①～④のうちから一つ選びなさい。

①　機密性，可用性，残存性

②　機密性，完全性，可用性

③　機密性，完全性，残存性

④　完全性，可用性，残存性

問２　情報セキュリティに対する組織の取り組みとして，情報資産の安全性を保つために作成した対応策や規定を何というか。最も適切なものを，次の①～④のうちから選びなさい。

①　情報セキュリティの CIA

②　情報セキュリティポリシー

③　セキュリティホール

④　ソーシャルエンジニアリング

問３　個人でもできる情報セキュリティの対策として，最も適切なものを，次の①～④のうちから選びなさい。

①　パスワードに生年月日や電話番号を使う

②　パスワードは覚えやすいようなるべく短いものにする

③　パスワードは複数のサービスで同じものを使う

④　アカウントに二段階認証を設定する

問 4　認証についてまとめた次の表について，次の各問いに答えなさい。

（ア）認証	ID とパスワードによる認証など，その情報を知っていればログインできる認証
（イ）認証	指紋認証など，身体的特徴や行動的特徴を用いて行う認証
（ウ）認証	スマートフォンに SMS で認証コードを送信するなど，本人しか持っていないもので行う認証

(1)　空欄（ア）に入る語句として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　所持　　②　生体
③　知識　　④　二要素

(2)　空欄（イ）に入る語句として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　所持　　②　生体
③　知識　　④　二要素

(3)　空欄（ウ）に入る語句として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　所持　　②　生体
③　知識　　④　二要素

第 1 講　情報社会と問題解決

PART1　社会の進展と情報技術

問 1　省略

問 2　人工知能（ロボット）の判断の責任（例 . 自動運転）など

PART2　情報とメディア

問 1　省略

問 2　左上のグラフから，人気が年々上昇しているように見えるが，実際には累積グラフであるため，年ごとの売り上げが増えているわけではない。など

PART3　知的財産権

問 1　②，③，⑤

問 2　保護される著作物か，著作権の及ぶ利用行為ではないか，など

PART4　個人情報とプライバシー

問 1　利用している駅，通っている高校（制服から特定），など

問 2　個人情報を抜き取ることが目的のアプリである可能性がある。

問 3　省略

PART5　情報セキュリティ

問 1　ID/PASS の設定を見直す。など

問 2　(1)　フィッシング詐欺の可能性がある。

(2)　詐欺を目的とした Web サイトで，入力した個人情報や金銭を騙し取られる可能性がある。

PART6　問題の発見と解決

問 1　ルールが守られないと：批判されるのが嫌で，新しい意見が出なくなる。など
これ以外に必要なルール：リーダーを決める。など

問 2　省略

問 3　省略

第1講　PART5　確認問題　解答

問 1　②

解説：

情報セキュリティとは，情報の機密性，完全性，可用性を確保することである。

問 2　②

解説：

組織（企業や学校など）の持つ情報資産の安全性を保つために，組織が作成する対応策や規定。外部からの脅威への対応だけではなく，組織内部の情報管理についても規定する。これを情報セキュリティポリシーという。

問 3　④

解説：

パスワードには類推されやすい文字列を使わないようにすること，パスワードの使いまわしを避けることが情報セキュリティの観点では重要である。また，より強固な対策としては，二段階の認証を行う「二段階認証」などを利用する方法もある。

問 4

(1)　③

解説：

このような認証を知識認証という。

(2)　②

解説：

このような認証を生体認証という。

(3)　①

解説：

このような認証を所持認証という。